Commission's Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554.

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012/13

Date filed: 2/27/14

Name of company covered by this certification: Nucentcom, Inc. (the "company")

Form 499 Filer ID: 826686 Nucentcom, Inc.

Name of signatory: S.K. Mohan

Title of signatory: CEO

I, S.K. Mohan, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*
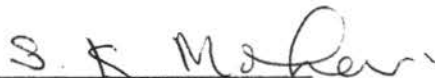
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed __S. K. Mohan_____

STATEMENT

The company adheres to the following policies and is fully compliant with the CPNI Certification requirement:

1.) Since 2011 the Company's business model did not require retention of PCI data. As that might change in the future the Company continues to adhere to the policies and procedures set forth above.

2.) Customer information is stored in a secured database on a server separately firewalled from all other production systems. Currently the company has no private information in the database of any individual.

3.) Access to customer information is highly restricted. Specifically, the information may be accessed only by: a.) certain accounting and finance personnel, and, b.) certain customer service personnel (and then in a very limited fashion).

4.) Customer information is not sold or distributed to any party under any circumstances.

5.) The only outside companies or individuals allowed access to the customer information are regulatory authorities and only upon submission of sufficient documentation to justify release of the information. The company's outside auditor has access to the ledger and customer data base but this access is limited to steps necessary to perform a financial audit.

6.) Database access is controlled in compliance with the PCI Data Security Standard.

7.) The Company has safeguards in place in the form of policies and procedures that assure that pretexting and other breaches will not occur.

8.) Customer call records are kept separate from customer address, contact, credit, payment and billing information (addressed previously). The customer call records are the only records made accessible online, and then only to the customers via password protection procedures consistent with the intent of the statutes.